REMARKS

This response is made in order to bring the application to allowance. It follows the paragraphs of the office action for ease of entering the amendments to the claims. Paragraphs from the office action are in italics and indented from the responses. A listing of the claims is provided as required in the new USPTO amendment practice per 37 CFR 1.121.

DETAILED ACTION

Claim Rejections - 35 USC § 101

Claim 23-28, 36-40 are rejected under 35 ASSOC.. 101 because claim 23 recites a method comprising: " generating a TCR commitment opening function for extracting a data string committed to by at least one TCR commitment message, utilizing a corresponding TCR opening string , and employing a TCR function and a regular commitment scheme used in generating TCR commitment message and used in generating corresponding TCR opening string". Steps of claim 23 is merely a series of function applied on various strings or messages with no concrete and tangible result.

In response, applicant respectfully states that in order to overcome the 101 rejection, claim 23 is amended to include the limitations of claims 32 and 34. Claims 32 and 34 are canceled. Thus claim 23 and claims that depend thereupon are allowable.

Dependent claims 32-34 are also rejected by virtue of their dependencies.
Apparatus claims 24-25 corresponding to method claims 23 are also rejected for the same reasons stated above.
Dependent claims 26-28, 36-40 are also rejected by virtue of their dependencies.

In response, applicant respectfully states that all these claim are allowable because of the allowance of claim 23 as amended.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 USC. 112: The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

***Claims 26-28, 31 and 37-40** are rejected under 35 USC. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.*

Claim 26 recites the limitation "said regular commitment scheme" in lines 20-21. There is insufficient antecedent basis for this limitation in the claim. Dependent claims 27-28 and 39 are rejected by virtue of their dependencies.

In response, applicant respectfully states that claim 26 is amended to depend upon method claim 10, and to change 'said regular commitment scheme' to 'a regular commitment scheme'. This overcomes the 112 rejection and claim 26, and claims 27, 28, and 39 which depend thereon are allowable.

Claims 26-28,37-40 are method claims depending from an apparatus claim 25 (computer program product). Dependent method claim should not be depending from a base method claim.

In response, applicant respectfully states that claim 2 as amended depends on method claim 10. This overcomes the 112 rejection and claim 26-28, and 37-40 which depend thereon are allowable.

Claims 31 and 35 recite "any TCR function" and "any regular commitment". The terms "any TCR function" and "any regular commitment" are not determinant and are relative terms which renders the claim indefinite. The specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

In response, applicant respectfully states that claims 31 and 35 are amended to include a portion of the limitation in claim 43. Claim 43 is amended to delete that portion included in claim 31., and to depend on claim 31. This overcomes the 112 rejection and makes claims 31 and 35 allowable.

Dependent claims 41-43 are rejected by virtue of their dependencies.

The amendments of claims 31 and 35 overcomes the 112 rejection and claim 41-43 which depend thereon are allowable.

Double Patenting

The non statutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See In re Goodman, 11 F.3d 1046,29 USPQ2d 2010 (Fed. Cir. 1993); In re Longi, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); In re Van Ornum, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); In re Vogel, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, In re Thorington, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1. 130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-9, 15, 17-18,20 and 21 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable Over claims], 6,] 2, 13.] 4, 18,46 and 60 of copending Application No. 09/307.493. Although the conflicting claims are not identical, they are not patentably distinct from each other because claim 1 of the copending application '493

is directed to a method of generating a signature for a message employing a public/private key pair in which the private key includes at least one enhancing key; and a public key which includes a TCR commitment (or a regular commitment recited in claim 12 of the Application '493) to at least one enhancing key recited in claims 1 and 3 of the pending application, see claim 1, lines 4-6.

In response, applicant respectfully states that although he takes exception with the Examiner's assertion that the present application suffers from, 'obviousness-type double patenting with regard to '493, in order to expedite allowance of the present application, a terminal disclaimer is included herewith.

Claim Rejections - 35 use § 102

The following is a quotation of the appropriate paragraphs of 35 US.C. 102 that form the basis for the rejections under this section made in this Office action: A person shall be entitled to a patent unless-(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 10, 44 and 29 are rejected under 35 US.C. 102(a) as being anticipated by M.Belare , P. Rogaway, Collision-Resistant Hashing: Towards making UOWHFs Practical, Department of Computer Science & Engineering, University of California at San Diego, July 1997. Belare teaches a signing with an TCR Hash family where the signing algorithm chooses K (i.e. a commitment) anew for each message (i.e. a first string). Belare further teaches that the key K is included with the signature. That is a second TCR function is applied to a second string that includes the commitment (i.e. key K), see pages 26-27, see also page 28. Belare discloses the steps of verifying a message using TCR function (i.e. a TCR de-commitment function) for verifying the TCR commitment message generated, see page 26.

Claim 44 is an apparatus corresponding to method claim 29. It is rejected for the same reasons stated in the statement of rejection of claim 29 above.

In response, applicant respectfully states that the following traverses the rejection of claims 10, 29 and 44 pursuant to 35 USC 102(a) as being anticipated by M. Bellare, P. Rogaway, Collision-Resistant Hashing: Towards making UOWHFs Practical, 1997, specifically pages 26, 27 and 28.

Whereas, the present invention is clearly based on the use of UOWFH's (or TCR functions) in a manner that is described in Bellare et. al., the above reference, the above reference and claims 10,29,44, are in regard to two entirely different cryptographic primitives. The reference deals with use of TCR functions for creating digital signatures while the present invention uses TCR functions for creating an entirely new and different cryptographic primitive called a TCR-commitment, as in claims 10, 29 and 44.

Digital Signatures and commitments (or TCR-commitments) are two very different cryptographic primitives. In a digital signature, the message that is signed is public knowledge and there is NO requirement that a signature hide all information about the value that is signed. In contrast a commitment or TCR-commitment by definition has to hide all information about the value that is committed (see Page 22 of application).

Bellare and Rogaway in pages 26, 27 and 28 are saying that for a message M (which may be public, or even chosen adversarially),

K, Sign(K || H_K(M))

represents a signature for message M , where K is a randomly chosen key K, H_K is a keyed TCR function and Sign is any digital signature function. Note that there is no requirement that Sign_K(K || H_K(M)) hide all information about M because M is expected to be public and even if it is not, for most signature schemes such as RSA, given the string Sign(K || H_K(M)) one can easily derive K and H_K(M) which easily constitutes information about M. For instance given only K and H_K(M) one can still determine that the unknown M is not the same as a known M' simply by computing H_K(M') and noting that it is different from

H_K(M). This constitutes leakage of information about M. In a more concrete example that makes this leakage clear, assume that M is a sealed bid for a contract then the Bellare-Rogaway signature, K, Sign(K|| H_K(M)) will not be suitable since if there were a small number (say n) of possibilities M1, M2, ..., Mn for the bid, anyone knowing K, Sign(K|| H_K(M)) can exhaustively test them all n of them and determine the actual bid.

In contrast the present invention is creating a TCR commitment using a regular commitment. Here we are using Sign(K || H_K(Commit(M)) as a TCR commitment for value of M. Note that knowing K and H_K(Commit(M)) gives no information about M since even knowing Commit(M) gives no information about M by the definition of a commitment function. Thus claims 10, 29 and 44 and all claims that depend thereupon are allowable over the cited art.

Allowable Subject Matter

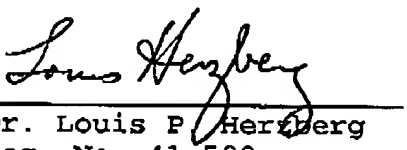
Claims 11-14, 16,19,22 and 30 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The amendments to the claims presented and described above overcome the rejections of the claims, and the objected-to claims 11-14, 16,19,22 and 30, which depend thereupon are allowable. Thus Claims 11-14, 16,19,22 and 30 are allowable.

It is anticipated that this amendment brings the application to allowance, and favorable action is respectfully solicited. In the unlikely event that any claim remains rejected, please contact the undersigned by phone in order to discuss the application.

Please charge any fee necessary to enter this paper to deposit account 09-0468.

Respectfully submitted,

By: 

Dr. Louis P. Herzberg
Reg. No. 41,500
Voice Tel. (914) 945-2885
Fax. (914) 945-3281

IBM CORPORATION
Intellectual Property Law Dept.
P.O. Box 218
Yorktown Heights, New York 10598